Introduction

Tadeusz Zieliński

Historically, humans have been, and continue to be, active in environments that have accompanied our species since its beginnings. We needed some time to discover these environments and learn how to manage them effectively. Initially, our primary natural environments were land and sea, but over time we also learned to fly, and eventually started to explore the outer space. For decades no one would expect that in addition to these three, and then four, domains, which are currently considered traditional, there is also a fifth—cyberspace, which permeates all the other. The discoverers of the electromagnetic field may have had an inkling that the waves they explored could form part of a new environment. But at that time no one used the term *cyberspace*, let alone being able to define it. Leaving aside the term itself, which emerged only in the second half of the twentieth century, cyberspace has become another area of exploration that is commonly considered to be interdisciplinary, and which at the same time is generating many new challenges, including especially those related to broadly defined security.

The significance of this new domain in the context of the security of both individuals and nations has become evident as technology continued to advance, ushering in computerisation in all its forms, and widespread access to the Internet. This direct access to information, available thanks to the rapid development of computer systems, is now one of the primary determinants of social and economic growth, and often determines the success or failure of an undertaking. Access to network services has influenced social relations and can be a tool for encouraging or controlling specific behavioural patterns, such as political decisions. Actions taken by various actors in cyberspace can directly produce specific economic, social, or political outcomes. This makes cyberspace an area that affects the security of the public and private sectors, and also that of citizens, and, by extension, of nations as a

T. Zieliński (✉)

Wydział Wojskowy/Faculty of Military Studies, Akademia Sztuki Wojennej
w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: t-zielinski@akademia.mil.pl

whole. Poland is no exception here, and it constantly articulates the importance of cyberspace for its national security in its National Security Strategy publications. The latest (2020) publication is no different, as its authors emphasise the role of cyberspace and information space in the social, economic, and military aspects. In this context, key postulates are to increase resilience to cyber risks and provide a better protection of public, military, and private information. Other worthwhile goals are to raise awareness and promote good practices so that citizens can protect their information better, and to create a safe information space for the state and society to function in. These objectives clearly show that cyberspace needs to be considered in terms of challenges and hazards, because these are what will constitute the blueprint for actions to ensure national security. This is also true for Poland, and it seems useful to see how the Polish national cybersecurity policy has developed in relation to these goals.

It is important to note that efforts to develop a comprehensive national strategy for counteracting security risks in cyberspace have been undertaken since 2008. By 2011, seven draft documents had been developed, but those were not adopted by the government, mainly because of poor content quality. The first strategic document on Poland's cybersecurity was Policy on Protecting the Cyberspace of the Republic of Poland (2013), as adopted by resolution of the Council of Ministers. While the document was designed to help achieve the appropriate level of security in cyberspace, it failed to identify any risks and only described them in general terms. As a result, the first systemic actions of government administration to identify the risks and challenges in cyberspace are those identified in *The Cybersecurity Doctrine of the Republic of Poland* (2015). That was the first document to describe the strategic directions and a shared vision for cybersecurity in relation to public administration units, security services, public order, and armed forces, but also the private sector and citizens. Of course, the question remains whether it was not too late for the state to address cyberspace security issues at the systemic level. Attacks in cyberspace, whether aimed at the public or private sectors, have happened virtually from the start of the computer revolution. But it was not until the cybernetic attack in 2007 on Estonia's critical infrastructure that many decision-makers realised that national security could be at risk and the components that are vital for state functioning could be paralysed. Therefore, the decision to adopt a systemic approach to cybersecurity by developing a consistent strategy, as found in *The Cybersecurity Doctrine of the Republic of Poland*, was certainly sensible but belated. Its authors divided challenges and risks into internal and external. When it comes to the former, these are considered similar to traditional risks and challenges, and differ only in terms of their environment and the tools that are used. This creates such categories as cybercrime, cyber violence, cyber protests, and destructive cyber demonstrations, which can disrupt some crucial functions within public administration and the private sector. The cyber risks that were considered particularly important were those related to state's critical infrastructure relying on computer systems. As regards internal challenges in cyberspace, special attention is given to legal loopholes and unregulated or poorly regulated relations between the individual members of the cybersecurity system. The authors of the Doctrine were right to note that this

problem might be exacerbated as individual elements of national, public, or private infrastructure become more dependent on computer systems. What seems interesting are conclusions drawn from the analysis of external risks and challenges. It was clearly shown that cyber conflicts and cyber crises involving national and non-national parties, including cyberwars, are likely to happen. In other words, cyberspace was considered among the domains which can serve as yet another battlefield for military operations. National security can also be compromised by cyber espionage involving foreign services and non-state parties, including terrorist organisations. As regards to challenges, there was apparently no shared terminology and definitions for allied cyberspace operations, which seems natural but needed addressing, as the allied cybersecurity system was only developing.

The next step in developing our national cybersecurity policy were efforts by the government administration to work out a cybersecurity strategy. Its first draft was completed in 2016, and a year later we adopted *The Cybersecurity Strategy of the Republic of Poland for 2017–2022*, also referred to as The National Framework of Cybersecurity Policy. That document did not identify any specific risks or challenges for Poland's cyberspace security, but this was not the objective behind the Strategy. In the context of risks, those are collectively referred to as cyber risks. The challenges that were considered crucial were

to ensure information safety across all members of the national cybersecurity system, i.e. businesses that provide their services using communication and information systems, as well as cyberspace users, public government authorities, and professional organisations dealing with ICT security in the operational domain.

The Cybersecurity Strategy identifies the primary goal, “to ensure a high level of security for the public and private sectors and for citizens in relation to providing or using essential services and digital services”, and four sub-goals,

(a) to achieve capability for nationally coordinated action to prevent, detect, fight, and mitigate the consequences of incidents that compromise the security of state's critical communication and information systems; (b) to enhance the capacity to prevent cyber risks; (c) to develop the national cyberspace security potential and expertise; (d) to position the Republic of Poland as a strong international player in cybersecurity.

Without going into details, it can be claimed that the Cybersecurity Strategy addresses some major issues, as found in similar documents prepared by other countries. Is it a complete document? Probably not, but at the time it was adopted (2017), it served as the basis for some more advanced work, including at the legal level, to make it a complete strategy in the future. Importantly, as the document was approved, experts argued that it needed to be quickly implemented, which was ultimately to translate into the development of the Act on Cybersecurity. Consequently, it was only natural that in 2018 the Minister of Digital Affairs presented an action plan referring to the National Framework of Cybersecurity Policy, a planning document to describe in detail how to achieve the sub-goals identified in the Cybersecurity Strategy. An important element of that document was also the division of responsibilities between the relevant government administration authorities.

Cybersecurity actions taken by government administration authorities ultimately made it possible for the Sejm, the Lower House of the Polish Parliament, to adopt in 2018 the Act on the National Cybersecurity System. This was the first legal Act in Poland to regulate this field. The goal of that regulation was to ensure cybersecurity in relation to the provision of essential services and digital services, and to define the rules for selecting the operators of essential services and defining their responsibilities in cybersecurity matters. The Act also defined the bodies in charge of cybersecurity, which are responsible for supervising the operators of essential services. In addition, the regulation describes the scope of the Cybersecurity Strategy of the Republic of Poland. Following the above, in 2019, Poland adopted *The Cybersecurity Strategy of the Republic of Poland for 2019–2024*.

The current Cybersecurity Strategy is similar to that adopted in 2017. What makes it different from its antecedent is the new vision which is to “continuously strengthen and develop the national cybersecurity system.” The new strategy seems to be more mature and more specific, also in relation to its goal and implementation details, which are “to increase resilience to cyber risks and improve the level of information protection in the public, military, and private sectors, as well as to promote good practices to help citizens better protect their information.” There is also a new, important sub-goal, namely to raise awareness and social expertise related to cybersecurity. Unfortunately, the government did not secure the funds to implement the tasks defined in the Cybersecurity Strategy. Its provisions are to be implemented from the budgets of individual units, and from the funds of the National Centre for Research and Development, and EU funds.

The presented overview of how Poland’s national cybersecurity policy has developed, and lessons learned from this demonstrate that the issues related to cybersecurity in its broad sense can be reduced to three key areas—technology, law and organisation, and society. These are complementary to one another and equally important.

There is no doubt that technology is an important area in preventing cyber risks. This is clearly articulated in the current Cybersecurity Strategy. Access to new technologies is accelerating globalisation, which in turn is generating further technological advancements. Cyberspace is an environment in which new technologies are crucial and determine the success of any endeavour. The transformation of society, through the development of computer technologies, into information society with access to cyberspace resources has produced more risks for nations and citizens. On the one hand, modern technology has contributed to improved cybersecurity, but on the other hand it can compromise the security of citizens and nations. Research and development, and technological advancements in cybersecurity, should definitely be aimed at enhancing Poland’s cyberspace security. These technologies should make it possible to detect, notify and protect us against the existing and future risks in cyberspace, and their consequences.

The second area, law and organisation, is directly associated with legal regulations on cybersecurity and with systemic solutions adopted in Poland. The national cybersecurity system has been functioning on the basis of the Act on the National Cybersecurity System, which also aligns Polish law with Directive 2016/1148 of the

European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, known as the NIS Directive. The main goal of this legislation is to ensure cybersecurity at the national level. The system relies on the operators of essential services, including from the energy, transport, health, and banking sectors, digital service providers, Computer Security Incident Response Teams (CSIRTs) at the national level, sectoral cybersecurity teams, cybersecurity service providers, responsible cybersecurity authorities, and single points of contact as part of the European Union cooperation on cybersecurity. Cybersecurity, understood as the resilience of computer systems to any action that compromises the confidentiality, integrity, availability or authenticity of processed data, or the related services offered by those systems, requires the appropriate organisation of the entities referred to in the Act. After the 2 years that the national cybersecurity system has been in operation (since 2018), it is possible to state that the undertaken actions have proven successful, and the development of a resilient system is a continuous process. Despite many difficulties and challenges along the way, the system has slowly become more and more methodical and informed, even though it still requires legislation adjustments to standardise the solutions used across the various sectors involved in its development. At the same time, an insufficient pool of well-qualified personnel and experts on cybersecurity requires further systemic solutions related to education and scientific research.

The social area of cybersecurity in Poland is directly associated with information society, often referred to as cybersociety. Similarly to other countries, in Poland society, meaning citizens, but also public organisations, is more and more dependent on technology and network services. By using the available network solutions, people, either consciously or unconsciously, share data about their lives, behaviour, and interests. As a result, they are increasingly vulnerable to risks which require “cyber awareness”. This, in turn, generates educational needs in this area related to the fundamentals of personal safety online, safe shopping and payments, safety of parents and children online, safe use of social media, and many more issues on which various social groups need to be educated. This generates demand for various types of educational services, which are expected to contribute to raising knowledge and social awareness, and, by extension, to improving state security. Cyberspace is also an environment where educational services can, and are, provided. This also applies to the public sphere, which should foster appropriate values and behaviour in cyberspace through educational activities. In the future, knowledge of technologies that protect our life in cyberspace should be common, especially given that we are heading towards becoming a cybersociety.

To sum up, the national cybersecurity system built in Poland plays an important part in improving national security in general. In addition to the other four domains, cyberspace is starting to serve a crucial role in security, which is only natural as our society is becoming a cybersociety. Of course, many questions remain unanswered, and not all of the challenges and risks in the area of cybersecurity can be anticipated. Nevertheless, the actions taken by the government administration in Poland to improve its cybersecurity system can be assessed positively.

Tadeusz Zieliński dr. hab., associate professor at the War Studies University in Warsaw, and vice rector for Scientific Affairs at WSU. Tadeusz Zieliński is a lecturer in the field of air power, unmanned aircraft systems, and global threats security. His scientific area of interest is defense and security, in particular the EU Common Security and Defense Policy and the theory and practice of the use of military aviation and unmanned (autonomous) air systems in conflicts and crisis response operations.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.